Landesamt für Sicherheit in
der Informationstechnik

LSI-Info T#05

INTRUSION-DETECTION-/ INTRUSION-PREVENTION-SYSTEM (IDS / IPS)

EIN ERGÄNZENDES SYSTEM ZUR NETZWERKÜBERWACHUNG

Version 1.0 vom: 25.06.2020

Management Summary

Ein Intrusion-Detection-System (IDS) ist ein System, das ein Netzwerk oder eine Netzwerkkomponente überwacht und verdächtige Aktivitäten wie Angriffe oder schadhafte Datenübertragung anhand von Mustern und Heuristik erkennen kann. Über die reine Erkennung hinaus kann ein Intrusion-Prevention-System (IPS) nicht nur verdächtige Aktivitäten anhand von Mustern erkennen, sondern auch aktiv abwehrende Maßnahmen einleiten. Ein IPS ist also ein IDS mit der Zusatzfunktion, aktiv einen laufenden Vorfall zu stoppen. IDS/IPS-Systeme sind unter anderem dazu gedacht, eine Firewall oder Antivirensoftware zu ergänzen, um die Sicherheit in einem Netzwerk zu erhöhen.

TECHNIKEN

Es gibt verschiedene Techniken, die einen zusätzlichen Schutz gewährleisten:

Einige IDS/IPS können Datenänderungen überwachen (Datenintegrität), indem diese auf dem jeweiligen Host installiert werden. Das Dateisystem des Hosts wird dabei anhand von Vorgaben des Administrators gescannt, Prüfsummen (Hashes) zu Dateien und Verzeichnissen erstellt und in einer Datenbank gespeichert. Nach einer festgelegten Zeit werden die gespeicherten Prüfsummen aus der Datenbank mit aktuellen Prüfsummen der Dateien im Dateisystem verglichen (Prüfsummenvergleich). Sollten sich Unterschiede ergeben, wird eine Alarm-Meldung erzeugt. Um eine Flut von Falschmeldungen zu vermeiden, sollte an dieser Stelle überlegt werden, welche Dateien sich häufig ändern z.B. Word-Dokumente und Log-Dateien, um diese ggfs. von vorneherein von der Prüfung auszuschließen.

Andere IDS/IPS überwachen Authentifikationslogs oder den Netzwerkverkehr. Bei der Überwachung der Authentifikationslogs wird das IDS/IPS beispielsweise auf dem jeweiligen Host installiert, auf dem die Logs überwacht werden sollen. Diese Logs werden dann auf fehlgeschlagene Login-Versuche überprüft und nach einer benutzerdefinierten Anzahl pro Zeiteinheit fehlgeschlagener Logins die Quell-IP des Angreifers gesperrt. Die Dauer der Sperrung wird dabei vom Administrator festgelegt.

Eine weitere Möglichkeit: IDS/IPS zur Überwachung einzelner Netzwerksegmente. Da sich das Monitoring auf ein Subnetz beschränkt und sich eine Überwachung in einer geswitchten Umgebung schwierig gestaltet, empfiehlt es sich, das IDS/IPS direkt hinter der Firewall zu positionieren, so dass der komplette ein- und ausgehende Netzwerkverkehr mitgelesen werden kann. Alternativ kann in einer geswitchten Umgebung über Agents auf den Endgeräten, oder über Port-Mirroring (nur IDS) gearbeitet werden.
Bei dieser Technik werden Datenpakete entweder mit charakteristischen Mustern (Signaturen) verglichen oder es wird auf heuristische Methoden zurückgegriffen. Bei der Signatur-Methode können nur bereits bekannte Bedrohungen gefunden werden, bei der heuristischen Methode hingegen können auch bisher unbekannte Bedrohungen gefunden werden, da das IDS/IPS hier lernt, Abweichungen vom regulären Betrieb zu erkennen. Bei dieser Methode werden also Muster im Datenstrom des Netzwerkverkehrs gelernt, um im Anschluss Anomalien zu identifizieren. Allerdings kann bei der

heuristischen Methode die Wahrscheinlichkeit von Falschmeldungen oder nicht gefundenen Bedrohungen hoch sein (False Positives und False Negatives).
Durch die Überwachung des Netzwerkverkehrs, können im Eintrittsfall neben einer reinen (IDS-)Alarmierung im IPS-Betriebsmodus auch IP-Adressen oder die Übertragung von Dateien im Netzwerk gesperrt werden.

ARTEN

Es gibt generell drei Arten von IDS/IPS: hostbasierte, netzwerkbasierte und hybride IDS/IPS. Hostbasierte Intrusion-Detection-Systeme / Intrusion-Prevention-Systeme (HIDS / HIPS) werden auf dem jeweiligen Host installiert, wodurch nur dieser überwacht wird. Das kann beispielsweise beim Überwachen der Datenänderungen und Authentifikationslogs der Fall sein.
Netzwerkbasierte Intrusion-Detection-Systeme / Intrusion-Prevention-Systeme (NIDS / NIPS) können in jedem Netzwerksegment auf einem Host installiert werden, wodurch das ganze Netzwerksegment überwacht werden kann. Next-Generation-Firewalls verfügen oftmals über NIDS-/NIPS-Funktionalitäten. Hybride IDS/IPS kombinieren die beiden vorherigen Arten, um eine höhere Abdeckung bei der Erkennung von Angriffen zu erzielen.

FUNKTIONSWEISE

Bei der Erkennung von Angriffen mit einem IDS/IPS System gibt es zwei Verfahren:

- Vergleich mit bekannten Angriffssignaturen
- Statistische Analyse (heuristische Methode)

Die Mehrheit dieser Systeme verwenden Signaturen, um Bedrohungen zu erkennen, wodurch nur bereits bekannte Angriffsmuster detektiert werden können. Die ständige Aktualisierung dieser Angriffsmuster ist ebenso bedeutsam wie die Aktualität der Virensignaturen beim Virenscanner. In der Regel erfolgt dies über den Abschluss einer Subscription beim Gerätekauf. Wurde eine Bedrohung erkannt, wird zuerst ein Alarm ausgelöst. Ein Alarm kann verschiedene Ereignisse auslösen, sei es eine E-Mail oder SMS an den Administrator oder ein Hinweistext auf der Konsole. Je nach Funktionsumfang des Systems kann dann automatisiert eine Sperrung oder Isolierung der vermeintlichen Bedrohung erfolgen (IPS).
Eine weitere Erkennungsmethode ist die statistische Analyse (heuristische Methode). Mit dieser könnten auch bisher unbekannte Angriffe ohne vorliegende Angriffsmuster

erkannt werden. Dabei steigt allerdings auch der Verwaltungsaufwand, da sehr genau geprüft werden muss, ob es sich im Einzelfall tatsächlich um eine Bedrohung handelt. Signaturbasierte Systeme haben den Vorteil, dass das Verhalten voraussehbar ist und leichter geprüft werden kann, ob es sich tatsächlich um eine Bedrohung handelt.
Einige IDS/IPS bieten verschiedene Zusatzfunktionen wie bspw. URL-Filter bzw. Prüfung der ein- und ausgehenden Mail-Attachments auf Basis des Dateisuffix des Anhangs.
Varianten von IDS/IPS besitzen die Funktionalität verschlüsselten Netzwerkverkehr zu inspizieren.

IMPLEMENTIERUNG

IDS/IPS Systeme können in Firewall- und Antivirenlösungen bereits vorhanden sein, alternativ als separate Hardware in einem Netzwerk bereitgestellt oder als Software auf einem Host eingesetzt werden. IDS/IPS gibt es sowohl als OpenSource-Lösungen, sowie als kommerzielle Produkte. Bei den Vorüberlegungen zur Einführung eines IDS/IPS sollte darauf geachtet werden, dass über den gesamten Einsatzzeitraum Sicherheits-Updates zur Verfügung stehen und genutzt werden können.

KONFIGURATION

Die richtige Konfiguration spielt bei IDS/IPS eine entscheidende Rolle, da u.a. vermieden werden sollte, dass unnötig viele „False Positives“ generiert werden. In der Regel bieten IDS/IPS verschiedene Reaktionsstufen an. Diese könnten sich bspw. von „kritisch“, „hoch“, „mittel“, „niedrig“ bis „informativ“ erstrecken. Gerade in der Einführungsphase gilt es, sich hier einer optimalen Konfiguration zu nähern. Ein besonderes Augenmerk ist auf die Einstufung anderer Sicherheitskomponenten durch das IDS/IPS zu legen. So könnte bspw. eine Verteilung von neuen Virensignaturen als Angriff eingestuft werden.

DATENSCHUTZ

Datenschutztechnisch muss geprüft werden, ob der Einsatz eines IDS/IPS im jeweiligen Netzwerksegment zulässig ist. Da bei der Analyse von Netzwerkpaketen auch sensible Daten gelesen und ggf. gespeichert werden können, kann es hier zu einer Verletzung von gesetzlichen Vorschriften und Mitbestimmungsrechten kommen. Besondere Sorgfalt ist bei der Inspizierung von verschlüsseltem Datenverkehr geboten.

Der Zugriff auf das IDS/IPS und der damit verbundene Zugang zu sensiblen Daten sollte sehr restriktiv gehandhabt werden, damit eine Manipulation des Systems verhindert wird, der Datenschutz gewahrt bleibt und keine Informationen über interne Abläufe ausgelesen werden können.

Es sollte vor dem Einsatz eines solchen Systems unbedingt der Datenschutzbeauftragte und die Personalvertretung hinzugezogen werden.

REFERENZEN

- DER.1 Detektion von sicherheitsrelevanten Ereignissen
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_1_Detektion_von_sicherheitsrelevanten_Ereignissen.html

- Intrusion-Detection und -Prevention-Systeme
  https://www.security-insider.de/intrusion-detection-und-prevention-systeme-a-735825/

KONTAKT

Weitere Informationen finden Sie unter:

https://lsi.bayern.de/kommunen/

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911/215 49 - 523 für Sie erreichbar.